8K

УДК 621.391:519.2:519.7

Л.В. Ковальчук[1], О.А. Сиренко[2]
[1] Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», г. Киев, Украина
[2] Киевский национальный университет имени Тараса Шевченко, г. Киев, Украина
lv_kov_crypto@mail.ru, Olga_Sirenko@ukr.net

Анализ перемешивающих свойств операций, заданных на одном носителе

В статье анализируется возможность применения атак гомоморфизма (групповых атак) к блочным шифрам в случае, когда в раундовых функциях используется чередование различных операций, таких как операции модульного и побитового сложения, модульного умножения. Получены результаты, характеризующие перемешивающие свойства операций побитового и модульного сложения на множестве двоичных векторов, а также результаты, характеризующие перемешивающие свойства операций сложения и умножения в кольце Z_{2^n}.

Введение

Основой обеспечения криптографической защиты информации с ограниченным доступом являются симметрические криптосистемы, среди которых наиболее широкое применение находят блочные шифры (БШ). Важнейшее требование к современным БШ – это практическая криптографическая стойкость относительно всех известных в настоящее время криптоаналитических атак.

Традиционный подход построения БШ основан на общепринятых принципах – рассеивании и перемешивании, сформулированных в основополагающей работе К. Шеннона [1]. Под рассеиванием подразумевается влияние одного знака открытого текста на многие знаки шифрованного текста, что позволяет «сгладить» статистические свойства открытых сообщений. Принципом перемешивания К. Шеннон назвал разрушение статистических зависимостей между открытым и шифрованным текстом при криптографическом преобразовании. Поэтому наиболее распространенным методом построения БШ на сегодняшний день является метод, основанный на применении так называемых итерационных схем, в которых шифрующие преобразования реализуются в виде суперпозиции достаточно простых преобразований (с точки зрения программной реализации и вычислительной сложности), каждое из которых вносит небольшой вклад в существенное суммарное рассеивание и перемешивание. Последовательность таких преобразований (примитивов), которая многократно повторяется в БШ, обычно называется раундом (циклом). Тогда необходимая криптографическая стойкость такого шифра достигается за счет применения большого числа простых преобразований, которые в совокупности обеспечивают «хорошие» перемешивающие и рассеивающие свойства.

Одним из общих требований к современным БШ является их обоснованная стойкость к аналитическим атакам, которые условно можно разделить на два больших класса – алгебраические и статистические методы криптоанализа. Алгебраические методы криптоанализа основаны на группировании открытых, шифрованных сообщений или ключей БШ в классы эквивалентных (или близких, в том или ином смысле) объектов, позволяющем понизить трудоемкость алгоритмов решения (размерность) соответствующих криптоаналитических задач. Стойкость БШ к подобным методам

криптоанализа, получившим в ряде публикаций название методов гомоморфизмов или группового криптоанализа [2], [3], как правило, определяется алгебраическими свойствами различных групп подстановок, связанных с системой раундовых шифрующих преобразований данного БШ.

В работе [4] рассматривалось действие операции сложения (умножения) в конечном поле на смежные классы относительно умножения (сложения). Было показано, что действие операции сложения (умножения) на элементы классов смежности относительно операции умножения (сложения) существенно разрушают структуру соответствующей факторгруппы. Исходя из полученных результатов, в указанной работе был сделан вывод о том, что использование композиции этих операций при построении алгоритма шифрования делает его стойким к криптоанализу на основе гомоморфизмов и позволяет проектировать итеративные шифры с использованием только операций в конечном поле, без необходимости реализовывать дополнительные примитивы [4-6].

В современных алгоритмах шифрования в раундовых функциях БШ гораздо чаще используются композиции таких операций, как операции модульного и побитового сложения, операция модульного умножения. Поэтому не менее актуальной и интересной задачей на сегодняшний день является задача исследования перемешивающих свойств этих групповых операций, носителем которых является множество двоичных векторов.

Целью данной работы является анализ возможности применения групповых атак (атак гомоморфизма) в случае, когда в раундовых функциях блочного шифра используется чередование различных операций, заданных на множестве двоичных векторов.

Вспомогательные обозначения

Введем следующие обозначения. Здесь и далее под $(V_n,\oplus)$ будем понимать множество векторов длины n с операцией побитового сложения, а под $(Z_{2^n},+)$ и $(Z^*_{2^n},\times)$ – аддитивную и мультипликативную группы кольца вычетов Z_{2^n}. Каждому целому числу $z \in Z_{2^n}$ поставим в соответствие битовый вектор длины n, который является двоичным представлением этого числа. Таким образом, отождествим множества Z_{2^n} и V_n. Целое число и соответствующий ему двоичный вектор будем обозначать одинаково, а из контекста будет понятно, какое именно представление используется.

Обозначение вида

$$\underbrace{\ldots}_{b_{k+1}\text{ бит}}\ \underbrace{0\ \ldots\ 0}_{a_k\text{ бит}}\ \underbrace{\ldots}_{b_k\text{ бит}}\ \ldots\ \underbrace{0\ \ldots\ 0}_{a_1\text{ бит}}\ \underbrace{\ldots}_{b_1\text{ бит}} \quad (1)$$

будем использовать для битового вектора длины $n=\sum_{i=1}^{k}a_i+\sum_{i=1}^{k+1}b_i$, у которого слева b_{k+1} произвольных бит, далее a_k нулевых бит и т.д.

Влияние операции модульного сложения на структуру факторгруппы $(V_n,\oplus)$ по ее подгруппе

Определение 1. Обозначим через $G(a_1,a_2,...,a_k;b_1,b_2,...,b_k,b_{k+1})$ подгруппу индекса 2^a группы $(V_n,\oplus)$, элементы которой содержат k «нулевых» блоков $A_1,...,A_k$, то есть имеют следующую структуру:

$$\underset{\text{блок } B_{k+1}}{\underbrace{\ldots}_{b_{k+1}\text{ бит}}}\ \underset{\text{блок } A_k}{\underbrace{0\ \ldots\ 0}_{a_k\text{ бит}}}\ \underset{\text{блок } B_k}{\underbrace{\ldots}_{b_k\text{ бит}}}\ \ldots\ \underset{\text{блок } A_2}{\underbrace{0\ \ldots\ 0}_{a_2\text{ бит}}}\ \underset{\text{блок } B_2}{\underbrace{\ldots}_{b_2\text{ бит}}}\ \underset{\text{блок } A_1}{\underbrace{0\ \ldots\ 0}_{a_1\text{ бит}}}\ \underset{\text{блок } B_1}{\underbrace{\ldots}_{b_1\text{ бит}}},$$

где биты из «ненулевых» блоков $B_1,...,B_{k+1}$ принимают произвольные значения, причем $\sum_{i=1}^{k} a_i = a$, $\sum_{i=1}^{k} b_i = b$ и $a+b+b_{k+1}=n,\ a_i>0,\ b_i>0$ при $i=2,...,k;\ b_1\ge 0$, $a_1>0$, $b_{k+1}\ge 0$.

Лемма 1. *В указанных обозначениях:*

а) все подгруппы в $(V_n,\oplus)$ имеют структуру

$$\underbrace{\ldots}_{b_{k+1}\text{ бит}}\ \underbrace{0\ \ldots\ 0}_{a_k\text{ бит}}\ \underbrace{\ldots}_{b_k\text{ бит}}\ \ldots\ \underbrace{0\ \ldots\ 0}_{a_2\text{ бит}}\ \underbrace{\ldots}_{b_2\text{ бит}}\ \underbrace{0\ \ldots\ 0}_{a_1\text{ бит}}\ \underbrace{\ldots}_{b_1\text{ бит}},$$

где $\sum_{i=1}^{k} a_i + \sum_{i=1}^{k+1} b_i = n,\ a_i>0,\ b_i>0$ при $i=2,...,k;\ b_1\ge 0$, $a_1>0$, $b_{k+1}\ge 0$;

б) все подгруппы в $(\mathbf{Z}_{2^n},+)$ имеют структуру

$$\underbrace{\ldots}_{n-k\text{ бит}}\ \underbrace{0\ \ldots\ 0}_{k\text{ бит}},$$

для некоторого $k=0,...,n$.

Теорема 1. *Пусть $G(a_1,a_2,...,a_k;b_1,b_2,...,b_k,b_{k+1})$ – некоторая подгруппа индекса 2^a группы $(V_n,\oplus)$; v_1 и v_2 – случайные элементы, равновероятно распределенные в классах смежности H_i и H_j подгруппы G, соответственно; $i,j=1,...,2^a$. Тогда:*

1) количество классов смежности по подгруппе G, в которые сумма элементов v_1 и v_2 по модулю 2^n попадает с ненулевой вероятностью, равно

$$2^k,\ \text{если } b_1>0,$$
$$2^{k-1},\ \text{если } b_1=0;$$

а количество классов смежности, в которые сумма элементов v_1 и v_2 по модулю 2^n попадает с нулевой вероятностью, равно

$$2^a-2^k,\ \text{если } b_1>0,$$
$$2^a-2^{k-1},\ \text{если } b_1=0;$$

2) если $H_i=H_j$, то классы смежности, в которые разность элементов v_1 и v_2 по модулю 2^n попадает с ненулевой вероятностью, имеют следующий вид:

$$\underset{\text{блок } B_{k+1}}{\underbrace{\ldots}_{b_{k+1}\text{ бит}}}\ \underset{\text{блок } A_k}{\underbrace{\ldots}_{a_k\text{ бит}}}\ \underset{\text{блок } B_k}{\underbrace{\ldots}_{b_k\text{ бит}}}\ \ldots\ \underset{\text{блок } B_2}{\underbrace{\ldots}_{b_2\text{ бит}}}\ \underset{\text{блок } A_1}{\underbrace{\ldots}_{a_1\text{ бит}}}\ \underset{\text{блок } B_1}{\underbrace{\ldots}_{b_1\text{ бит}}},$$

где блоки A_l содержат либо только 0, либо 1, для любого $l=1,...,k$, и количество этих классов смежности равно

$$2^k,\ \text{если } b_1>0,$$
$$2^{k-1},\ \text{если } b_1=0;$$

а количество классов смежности, в которые разность элементов v_1 и v_2 по модулю 2^n попадает с нулевой вероятностью, равно

$$2^a - 2^k\text{, если } b_1 > 0,$$

$$2^a - 2^{k-1}\text{, если } b_1 = 0.$$

При этом вероятности попадания разности элементов v_1 и v_2 в различные классы смежности будут одинаковые при любом выборе класса смежности H_i (т.е. класса смежности, которому принадлежат v_1 и v_2) и будут зависеть только от вида подгруппы, по которой строятся эти классы смежности;

3) ненулевые вероятности попадания суммы (разности) элементов v_1 и v_2 по модулю 2^n в соответствующие классы смежности будут лежать в пределах от $\prod_{i=1}^{k} q_{b_i}$ до $\prod_{i=1}^{k} p_{b_i}$.

Следует отметить, что если в подгруппе только «нулевые» блоки единичной длины, то количество классов смежности, в которые сумма векторов по модулю 2^n попадает с ненулевой вероятностью, будет наибольшим. Если же «нулевые» блоки будут большой длины, то количество классов смежности, в которые сумма векторов по модулю 2^n будет попадать с ненулевой вероятностью, уменьшается. Чем длиннее будут «нулевые» блоки, тем в меньшее количество классов смежности попадает сумма векторов по модулю 2^n с ненулевой вероятностью, то есть перемешивающие свойства операции модульного сложения относительно побитового сложения будут зависеть от структуры подгруппы.

Влияние операции побитового сложения на структуру факторгруппы $(\mathbf{Z}_{2^n},+)$ по ее подгруппе

Теорема 2. *Пусть G_k – подгруппа $(\mathbf{Z}_{2^n},+)$ индекса 2^k. Тогда:*

1) G_k (в соответствующем представлении) – подгруппа $(V_n,\oplus)$;

2) классы смежности по подгруппе G_k (относительно операции +) имеют вид $i+G_k$, $0 \le i < 2^k$;

3) классы смежности по подгруппе G_k (относительно операции $\oplus$) имеют вид $i \oplus G_k$, причем $i \oplus G_k = i + G_k$, $0 \le i < 2^k$;

4) если $v_1, v_2 \in i + G_k$, то с вероятностью 1 $v_1 \oplus v_2 \in G_k$; $0 \le i < 2^k$;

5) если $v_1, v_2 \in i \oplus G_k$, то с вероятностью 1 $v_1 - v_2 \in G_k$; $0 \le i < 2^k$;

6) если $v_1 \in i + G_k$, $v_2 \in j + G_k$, то с вероятностью 1 $v_1 \oplus v_2 \in i \oplus j + G_k$, причем класс смежности $i \oplus j + G_k$, вообще говоря, не совпадает с $i + j + G_k$, $0 \le i, j < 2^k$;

7) если $v_1 \in i \oplus G_k$, $v_2 \in j \oplus G_k$, то с вероятностью 1 $v_1 + v_2 \in i + j + G_k$; $0 \le i, j < 2^k$.

Из данной теоремы можно сделать следующий вывод: если подгруппа имеет структуру, описанную в п. б) леммы 1, то есть для некоторого $k = 0,...,n$ элементы этой подгруппы имеют следующий вид

$$\underbrace{...}_{n-k \text{ бит}}\underbrace{0 \ \ ... \ \ 0}_{k \text{ бит}},$$

то операция побитового (модульного) сложения сохраняет структуру соответствующей факторгруппы относительно модульного (побитового) сложения.

Анализ перемешивающих свойств операции умножения по модулю 2^n на классах смежности, построенных по группе $(Z_{2^n},+)$

Лемма 2. *О структуре группы* $(Z_{2^n},+)$*:*

1) Группа $(Z_{2^n},+)$ *– циклическая группа, генераторами которой будут все непарные числа от* 1 *до* 2^n-1.

2) Все подгруппы группы $(Z_{2^n},+)$ *в битовом представлении имеют вид:*

$$H_k = \left\{a \cdot 2^k, 0 \le a \le 2^{n-k}-1\right\},$$

то есть каждый элемент из H_k *имеет следующий вид:*

$$\underbrace{...}_{n-k \text{ бит}}\underbrace{0 \ \ ... \ \ 0}_{k \text{ бит}},$$

для $k = 0,...,n$.

Рассмотрим группу $(Z_{2^n},+)$. Все ее подгруппы будут иметь порядки 2^{n-k}, $k = 0,...,n$, а индексами соответственно будут числа 2^k, $k = 0,...,n$.

Рассмотрим подгруппу H группы $(Z_{2^n},+)$, индекс которой равен 2^k. Элементы этой подгруппы в битовом представлении будут иметь следующий вид:

$$\underbrace{...}_{n-k \text{ бит}}\underbrace{0 \ ... \ 0}_{k \text{ бит}}.$$

Выпишем все классы смежности по подгруппе H:

$$H_1 = 0 + H = \{2^k \cdot l,\ l = 0,...,2^k-1\};$$
$$H_2 = 1 + H = \{2^k \cdot l + 1,\ l = 0,...,2^k-1\};$$
$$\dots$$
$$H_{2^k} = 2^k - 1 + H = \{2^k \cdot l + 2^k - 1,\ l = 0,...,2^k-1\}.$$

Теорема 3. *Пусть* H *– подгруппа группы* $(Z_{2^n},+)$ *порядка* 2^{n-k} *и индекса* 2^k, $k = 0,...,n$*;* v_1 *и* v_2 *– случайные элементы, которые равновероятно распределены в классах смежности* $i+H$ *и* $j+H$*, где* $i, j \in \left\{0,..,2^k-1\right\}$*, соответственно. Тогда*

$$P\left(v_1 \cdot v_2 \in i \cdot j \left(\bmod 2^k\right) + H \Big/ v_1 \in i + H;\ v_2 \in i + H \right) = 1, \text{ где } i, j \in \left\{0,..,2^k-1\right\}.$$

Из полученных результатов можно сделать вывод, что операция умножения практически не разрушает структуру факторгруппы аддитивной группы $(Z_{2^n},+)$, другими словами, операция модульного умножения относительно операции модульного сложения будет обладать плохими перемешивающими свойствами.

Анализ перемешивающих свойств операции сложения по модулю 2^n на классах смежности, построенных по группе $(Z^*_{2^n},\times)$

Лемма 3. *О структуре группы* $(Z^*_{2^n},\times)$*:*

1) группа $(Z^*_{2^n},\times)$ *не будет циклической при* $n\geq 3$*;*

2) элемент данной группы $g=5$ *порождает ее циклическую подгруппу следующего вида:*

$$G=\{u\in Z^*_{2^n} : u=4k+1, k\in N\};$$

3) эта подгруппа будет максимальной в том смысле, что если для некоторой подгруппы G_1 *выполняется:* $G_1\subset G$ *и* $G_1\neq G$*, то* $G_1=Z^*_{2^n}$.

Теорема 4. *Пусть* H *– подгруппа группы* $(Z^*_{2^n},\times)$ *порядка* $k=2,...,2^{n-2}$ *и соответствующего индекса* $m=2^{n-2},...,2$*;* $H_1,...,H_m$ *– соответствующие классы смежности по подгруппе* H*;* v_1 *и* v_2 *– случайные элементы, которые равновероятно распределены в этих классах смежности* H_i *и* H_j*, где* $i,j\in\{1,...,m\}$*, соответственно. Тогда*

$$P\left(v_1+v_2\in H_l \middle/ v_1\in H_i;\ v_2\in H_j\right)=0,\ \text{где}\ i,j,l\in\{1,...,m\}.$$

Из полученных результатов можно сделать вывод, что операция модульного сложения относительно операции модульного умножения будет также обладать плохими перемешивающими свойствами. Другими словами, операция сложения в кольце Z_{2^n} не разрушает структуру факторгруппы мультипликативной группы кольца, построенной по ее любой подгруппе.

Выводы

Результаты, полученные в данной работе, характеризуют перемешивающие свойства операций побитового и модульного сложения, а также операций модульного сложения и умножения, заданных на одном носителе.

Наиболее интересным является тот факт, что действие операции модульного сложения на факторгруппу относительно операции побитового сложения существенно зависит от выбора подгруппы в $(V_n,\oplus)$, а действие операции побитового сложения сохраняет структуру соответствующей факторгруппы по любой подгруппе в $(Z_{2^n},+)$. Операция умножения в кольце Z_{2^n} практически не разрушает структуру факторгруппы его аддитивной группы (по любой подгруппе). Аналогичное утверждение будет справедливо также и для операции сложения в этом кольце.

Данный факт дает потенциальную возможность применять атаку гомоморфизмов (групповую атаку) при некоторых дополнительных условиях в том случае, когда в раундовых функциях блочного шифра используется чередование этих операций.

Литература

1. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике / К. Шеннон. – М. : Издательство иностранной литературы, 1963. – С. 333-402.
2. Paterson K.G. Imprimitive permutation groups and trapdoors in iterated block ciphers / K.G. Paterson // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 201-214.
3. Wagner D. Towards a unifying view of block cipher cryptanalysis / D. Wagner // Fast Software Encryption. – FSE'04, Proceedings. – Springer Verlag, 2004. – P. 116-135.
4. Шемякина О.В. О перемешивающих свойствах операций в конечном поле / О.В. Шемякина // Труды Восьмой Общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-09), (30 октября – 2 ноября 2009). – М. : МЦНМО, 2010. – Т. 2. – С. 87-90.
5. Горчинский Ю.Н. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями / Ю.Н. Горчинский // Труды по дискретной математике. – М. : ТВП, 1997. – Т. 1. – С. 67-84.
6. Горчинский Ю.Н. Стохастические алгебры / Ю.Н. Горчинский // Труды по дискретной математике. – М. : ТВП, 1998. – Т. 2. – С. 55-87.

Literatura

1. Shennon K. Rabotypoteoriiinformacii i kibernetike. M.: Izdatel'stvoinostrannojliteratury. 1963. S. 333-402.
2. Paterson K.G. FastSoftwareEncryption. FSE'99, Proceedings. SpringerVerlag. 1999. P. 201-214.
3. Wagner D. FastSoftwareEncryption. FSE'04, Proceedings. SpringerVerlag. 2004. P. 116-135.
4. Shemjakina O.V. TrudyVos'mojObshherossijskojnauchnojkonferencii «Matematika i bezopasnost' informacionnyh tehnologij» (MaBIT-09), 30 oktjabrja – 2 nojabrja 2009. T. 2. M. : MCNMO. 2010. S. 87-90.
5. GorchinskijJu.N. Trudypodiskretnojmatematike. T 1. M.: TVP. 1997. S. 67-84.
6. GorchinskijJu.N. Trudypodiskretnojmatematike. T 2. M. : TVP. 1998. S. 55-87.

Л.В. Ковальчук, О.О. Сіренко

Аналіз перемішувальних властивостей операцій, визначених на одному носії

У статті аналізується можливість застосування атак гомоморфізмів (групових атак) до блочних шифрів у випадку, коли в раундових функціях використовується чергування різних операцій, таких як операції модульного та побітового додавання, а також модульного множення. Отримані результати, які характеризують перемішувальні властивості операцій побітового та модульного додавання на множині двійкових векторів, а також результати, що характеризують перемішувальні властивості операцій додавання та множення в кільці Z_{2^n} .

L. Kovalchuk, O. Sirenko

Analysis of Mixing Features of the Operations, Defined on One Carrier

The paper is devoted to the analysis of the possibility of homomorphism attacks (group attack) to the block cipher in the case when the round functions use the interchange of various operations such as bitwise and modular addition, modular multiplication. Some results characterizing the mixing properties of bitwise and modular addition on the set of binary vectors and the results that characterize the mixing properties of addition and multiplication in the ring Z_{2^n} are obtained.

Статья поступила в редакцию 08.07.2011.